

**IN THE CLAIMS:**

1 1. (CURRENTLY AMENDED) A method for implementing port-based network access  
2 control at a shared media port in an intermediate node, the shared media port being cou-  
3 pled to a plurality of client nodes, the method comprising:  
4 partitioning the shared media port into a plurality of logical subinterfaces, each  
5 logical subinterface dedicated to providing access to a different network or subnetwork  
6 accessible through the intermediate node;  
7 receiving a data packet at the shared media port from a first client node;  
8 associating the received data packet with a first logical subinterface in the plural-  
9 ity of logical subinterfaces;  
10 determining whether the first client node is authenticated to communicate over the  
11 first logical subinterface's dedicated network or subnetwork; ~~and~~  
12 if the first client node is determined to be authenticated to communicate over the  
13 first logical subinterface's dedicated network or subnetwork, forwarding the received  
14 data packet over the first logical subinterface's dedicated network or subnetwork;  
15 receiving a second data packet at the shared media port from a second client node;  
16 associating the second received data packet with the first logical subinterface;  
17 determining whether the second client node is authenticated to communicate over  
18 the first logical subinterface's dedicated network or subnetwork; and  
19 if the second client node is determined to not be authenticated to communicate  
20 over the first logical subinterface's dedicated network or subnetwork, preventing the sec-  
21 ond received data packet from being forwarded over the first logical subinterface's dedi-  
22 cated network of subnetwork, while still allowing data packets from the first client node  
23 to be forwarded if the first client node is determined to be authenticated.

1 2. (ORIGINAL) The method according to claim 1, further comprising:  
2 performing at least one of dropping the received data packet or reclassifying the  
3 received data packet to a different logical subinterface, if the first client node is deter-

4 mined not to be authenticated to communicate over the first logical subinterface's dedi-  
5 cated network or subnetwork.

1 3. (ORIGINAL) The method according to claim 1, wherein the first logical subinterface's  
2 dedicated network or subnetwork is a virtual private network (VPN).

1 4. (ORIGINAL) The method according to claim 1, wherein a logical subinterface in the  
2 plurality of logical subinterfaces is dedicated to providing access to the Internet.

1 5. (ORIGINAL) The method according to claim 1, wherein the step of determining  
2 whether the first client node is authenticated to communicate over the first logical subin-  
3 terface's dedicated network or subnetwork further comprises:  
4 parsing a source media access control (MAC) address from the received data  
5 packet;  
6 indexing an entry in a MAC filter associated with the shared media port based on  
7 the value of the parsed source MAC address;  
8 identifying an authentication state stored in the indexed MAC-filter entry; and  
9 determining whether the first client node is authenticated to communicate over the  
10 first logical subinterface's dedicated network or subnetwork based on the authentication  
11 state stored in the indexed MAC-filter entry.

1 6. (ORIGINAL) The method according to claim 5, wherein the MAC filter is organized  
2 as a hash table.

1 7. (ORIGINAL) The method according to claim 1, further comprising:  
2 parsing a destination Internet Protocol (IP) address from the received data packet;  
3 comparing the parsed destination IP address to one or more IP addresses stored in  
4 an IP filter associated with the shared media port; and

5 if the parsed destination IP address matches an IP address stored in the IP filter,  
6 forwarding the received data packet over the first logical subinterface's dedicated net-  
7 work or subnetwork, even if the first client node is determined not to be authenticated to  
8 communicate over that network or subnetwork.

1 8. (ORIGINAL) The method according to claim 1, wherein the step of associating the  
2 received data packet with the first logical subinterface, further comprises:  
3 locating an entry in a routing table configured to store routing information associ-  
4 ated with the received data packet; and  
5 associating the received data packet with the first logical subinterface based on  
6 the contents of the routing-table entry.

1 9. (ORIGINAL) The method according to claim 1, further comprising:  
2 receiving an authentication request from the first client node at the shared media  
3 port;  
4 in response to receiving the authentication request, creating a MAC filter associ-  
5 ated with the shared media port if the MAC filter has not already been created;  
6 copying a source MAC address stored in the received authentication request into  
7 an appropriate entry in the MAC filter;  
8 forwarding the received authentication request to an authentication service;  
9 receiving a response from the authentication service, the response identifying an  
10 authentication state associated with the first client node; and  
11 storing the authentication state into the same MAC-filter entry into which the  
12 source MAC address was copied.

1 10. (ORIGINAL) The method according to claim 9, wherein the step of copying the  
2 source MAC address into an appropriate MAC-filter entry further comprises:  
3 indexing an entry in the MAC filter based on the result of applying a hash func-  
4 tion to the source MAC address; and

5 storing the source MAC address at the indexed MAC-filter entry.

1 11. (ORIGINAL) The method according to claim 9, wherein the received authentication  
2 request is an 802.1X authentication request.

1 12. (ORIGINAL) The method according to claim 9, further comprising:  
2 sending an alarm message over the first logical subinterface's dedicated network  
3 or subnetwork after the first client node fails to authenticate at the shared media port a  
4 predetermined number of times.

1 13. (ORIGINAL) The method according to claim 9, further comprising:  
2 sending an alarm message over the first logical subinterface's dedicated network  
3 or subnetwork after the first client node's authentication state changes from an authenti-  
4 cated state to an unauthenticated or unknown state.

1 14. (CURRENTLY AMENDED) An intermediate node for implementing port-based  
2 network access control in a network containing a plurality of client nodes, the intermedi-  
3 ate node comprising:  
4 a processor;  
5 a shared media port for receiving a data packet from a first client node, and a sec-  
6 ond data packet from a second client node, in the plurality of client nodes; and  
7 a memory adapted to store instructions for execution by the processor, at least a  
8 portion of the instructions defining a network operating system configured to perform the  
9 steps of:

10 partitioning the shared media port into a plurality of logical subinterfaces,  
11 each logical subinterface dedicated to providing access to a different network or  
12 subnetwork accessible through the intermediate node;  
13 associating the data packet received from the first client node with a first  
14 logical subinterface in the plurality of logical subinterfaces;

15                   determining whether the first client node is authenticated to communicate  
16                   over the network or subnetwork to which the first logical subinterface provides  
17                   dedicated access; ~~and~~  
18                   forwarding the received data packet over the first logical subinterface's  
19                   dedicated network or subnetwork only if the first client node is determined to be  
20                   authenticated to communicate over that network or subnetwork;  
21                   associating the second received data packet with the first logical subinter-  
22                   face;  
23                   determining whether the second client node is authenticated to communi-  
24                   cate over the first logical subinterface; and  
25                   preventing the second received data packet from being forwarded over the  
26                   first logical subinterface's dedicated network or subnetwork if the second client  
27                   node is determined to not be authenticated to communicate over that network or  
28                   subnetwork, while still allowing data packets from the first client node to be for-  
29                   warded over that network or subnetwork if the first client node is determined to be  
30                   authenticated.

1    15. (ORIGINAL) The intermediate node according to claim 14, wherein:  
2                   the memory is further adapted to store a MAC filter containing one or more en-  
3                   tries configured to store at least a MAC address and an authentication state, and  
4                   the network operating system is further configured to perform the steps:  
5                               receiving an authentication request from the first client node at the  
6                               shared media port;  
7                               copying a source MAC address stored in the received authentica-  
8                               tion request into an appropriate entry in the MAC filter;  
9                               forwarding the received authentication request to an authentication  
10                              service;  
11                              receiving a response from the authentication service, the response  
12                              identifying an authentication state associated with the first client node; and

13                   storing the authentication state into the same MAC-filter entry into  
14                   which the source MAC address was copied.

1    16. (ORIGINAL) The intermediate node according to claim 14, wherein:  
2           the memory is further adapted to store an IP filter containing a list of IP addresses,  
3    and  
4           the network operating system is further configured to perform the steps:  
5                   parsing a destination IP address from the received data packet;  
6                   comparing the parsed destination IP address to one or more IP ad-  
7                   dresses stored in an IP filter associated with the shared media port; and  
8                   if the parsed destination IP address matches an IP address stored in  
9                   the IP filter, forwarding the received data packet over the first logical sub-  
10                  interface's dedicated network or subnetwork, even if the first client node is  
11                  determined not to be authenticated to communicate over that network or  
12                  subnetwork.

1    17. (ORIGINAL) The intermediate node according to claim 14, wherein:  
2           the memory is further adapted to store a MAC filter containing one or more en-  
3    tries configured to store at least a MAC address and an authentication state, and  
4           the network operating system is further configured to perform the steps:  
5                   parsing a source MAC address from the received data packet;  
6                   indexing an entry in a MAC filter associated with the shared media  
7                   port based on the value of the parsed source MAC address;  
8                   identifying an authentication state stored in the indexed MAC-filter  
9                   entry; and  
10                  determining whether the first client node is authenticated to com-  
11                  municate over the first logical subinterface's dedicated network or sub-  
12                  network based on the authentication state stored in the indexed MAC-filter  
13                  entry.

1 18. (CURRENTLY AMENDED) An apparatus that implements port-based network ac-  
2 cess control at a shared media port, the shared media port being coupled to a plurality of  
3 client nodes, the apparatus comprising:

4 means for partitioning the shared media port into a plurality of logical subinter-  
5 faces, each logical subinterface dedicated to providing access to a different network or  
6 subnetwork accessible through the intermediate node;

7 means for receiving a data packet at the shared media port from a first client node;

8 means for associating the received data packet with a first logical subinterface in  
9 the plurality of logical subinterfaces;

10 means for determining whether the first client node is authenticated to communi-  
11 cate over the first logical subinterface's dedicated network or subnetwork; and

12 means for forwarding the received data packet over the first logical subinterface's  
13 dedicated network or subnetwork;

14 means for receiving a second data packet at the shared media port from a second  
15 client node;

16 means for associating the second received data packet with the first logical subin-  
17 terface;

18 means for determining whether the second client node is authenticated to commu-  
19 nicate over the first logical subinterface's dedicated network or subnetwork; and

20 means for preventing the second received data packet from being forwarded over  
21 the first logical subinterface's dedicated network of subnetwork, while still allowing data  
22 packets from the first client node to be forwarded.

1 19. (ORIGINAL) The apparatus according to claim 18, wherein the means for determin-  
2 ing whether the first client node is authenticated to communicate over the first logical  
3 subinterface's dedicated network or subnetwork further comprises:

4 means for parsing a source MAC address from the received data packet;

5 means for indexing an entry in a MAC filter associated with the shared media port  
6 based on the value of the parsed source MAC address;

7 means for identifying an authentication state stored in the indexed MAC-filter en-  
8 try; and

9 means for determining whether the first client node is authenticated to communi-  
10 cate over the first logical subinterface's dedicated network or subnetwork based on the  
11 authentication state stored in the indexed MAC-filter entry.

1 20. (ORIGINAL) The apparatus according to claim 18, further comprising:

2 means for parsing a destination IP address from the received data packet;

3 means for comparing the parsed destination IP address to one or more IP ad-  
4 dresses stored in an IP filter associated with the shared media port; and

5 means for forwarding the received data packet over the first logical subinterface's  
6 dedicated network or subnetwork, even if the first client node is determined not to be au-  
7 thenticated to communicate over that network or subnetwork.

1 21. (ORIGINAL) The apparatus according to claim 18, wherein the means for associating  
2 the received data packet with the first logical subinterface, further comprises:

3 means for locating an entry in a routing table configured to store routing informa-  
4 tion associated with the received data packet; and

5 means for associating the received data packet with the first logical subinterface  
6 based on the contents of the routing-table entry.

1 22. (ORIGINAL) The apparatus according to claim 18, further comprising:

2 means for receiving an authentication request from the first client node at the  
3 shared media port;

4 means for creating a MAC filter associated with the shared media port if the MAC  
5 filter has not already been created;

6 means for copying a source MAC address stored in the received authentication  
7 request into an appropriate entry in the MAC filter;



8 means for forwarding the received authentication request to an authentication ser-  
9 vice;

10 means for receiving a response from the authentication service, the response iden-  
11 tifying an authentication state associated with the first client node; and

12 means for storing the authentication state into the same MAC-filter entry into  
13 which the source MAC address was copied.

1 23. (ORIGINAL) The apparatus according to claim 22, wherein the received authentica-  
2 tion request is an 802.1X authentication request.

1 24. (CURRENTLY AMENDED) A computer-readable media including instructions for  
2 execution by a processor, the instructions for a method of implementing port-based net-  
3 work access control at a shared media port in an intermediate node, the shared media port  
4 being coupled to a plurality of client nodes, the method comprising the steps:

5 partitioning the shared media port into a plurality of logical subinterfaces, each  
6 logical subinterface dedicated to providing access to a different network or subnetwork  
7 accessible through the intermediate node;

8 receiving a data packet at the shared media port from a first client node;

9 associating the received data packet with a first logical subinterface in the plural-  
10 ity of logical subinterfaces;

11 determining whether the first client node is authenticated to communicate over the  
12 first logical subinterface's dedicated network or subnetwork; ~~and~~

13 if the first client node is determined to be authenticated to communicate over the  
14 first logical subinterface's dedicated network or subnetwork, forwarding the received  
15 data packet over the first logical subinterface's dedicated network or subnetwork;

16 receiving a second data packet at the shared media port from a second client node;  
17 associating the second received data packet with the first logical subinterface;  
18 determining whether the second client node is authenticated to communicate over  
19 the first logical subinterface's dedicated network or subnetwork; and  
20 if the second client node is determined to not be authenticated to communicate  
21 over the first logical subinterface's dedicated network or subnetwork, preventing the sec-  
22 ond received data packet from being forwarded over the first logical subinterface's dedi-  
23 cated network or subnetwork, while still allowing data packets from the first client node  
24 to be forwarded if the first client node is determined to be authenticated.

1 25. (NEW) An apparatus comprising:

2 a shared media port having a trusted subinterface configured to provide access to  
3 a trusted network or subnetwork and an untrusted subinterface configured to provide ac-  
4 cess to an untrusted network or subnetwork;

5 an authenticator configured to receive authentication requests from a plurality of  
6 client nodes and in response the authentication requests to independently assign to each  
7 of the plurality of client nodes an authentication state;

8 a media access control (MAC) filter configured to maintain an entry for each cli-  
9 ent node indicating the authentication state of the client node and a MAC address of the  
10 client node, and in response to receipt of a data packet from a particular client node di-  
11 rected to the trusted subinterface, to index to an entry of the MAC filter based on a source  
12 MAC address of the data packet, to identify the authentication state of the particular cli-  
13 ent node stored in the indexed MAC-filter entry, and to determine whether the particular  
14 client node is authenticated to communicate over the trusted subinterface, and, if so, to  
15 permit the particular client node to access the trusted subinterface,

16 wherein the media access control (MAC) filter grants client nodes access on a ba-  
17 sis client-by-client basis.

1 26. (NEW) The apparatus of claim 25, wherein the media access control (MAC) filter is  
2 further configured to redirect a data packet of the particular client node from the trusted  
3 subinterface to the untrusted subinterface if the particular client node is not authenticated  
4 to communicate over the trusted subinterface.

1 27. (NEW) The method according to claim 1, wherein the trusted network or subnetwork  
2 is a virtual private network (VPN).

1 28. (NEW) The method according to claim 1, wherein the untrusted network or subnet-  
2 work is the Internet.